



DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD
FORT BELVOIR, VIRGINIA 22060-6221

MAR 28 2006

IN REPLY J-61
REFER TO

MEMORANDUM FOR DIRECTOR, J6F

SUBJECT: Approval to Operate (ATO) for Business Systems Modernization – Energy (BSM-E)
Base Level Support Application (BLSA) Version 2.0 Type Accreditation

As the Designated Approving Authority for Defense Logistics Agency corporate systems, I am issuing BSM-E BLSA Version 2.0 Type Accreditation a 3-year ATO to expire on March 15, 2009. This ATO supports Type Accreditation for all BSM-E BLSA Version 2.0 host sites that have met minimum security requirements stipulated in the BSM-E BLSA Version 2.0 System Security Authorization Agreement (SSAA). This accreditation is applicable only to the Defense Energy Support Center standard configuration provided to the hosting sites. If there are any modifications made to this configuration, the host sites will be responsible for performing a separate certification and accreditation.

During the period of this accreditation, the following actions must be completed to ensure effective security controls are in place to protect BSM-E BLSA Version 2.0 resources:

- a. Annual SSAA Maintenance: This is an ongoing task to keep the SSAA current with all changes to the system mission, information sensitivity, threat, operating environment, security architecture, accreditation boundary, or operating procedures.
- b. Physical, Personnel, and Management Control Review: Periodic analysis of the operational procedures for the information system, such as addressing environmental concerns, personnel security controls, and physical security to identify any unacceptable risks to the information processed.
- c. Configuration Management: Continually assess proposed changes to the system to determine any potential impact to the security posture of the accredited system.
- d. Risk Management Review: Periodically assess the operation of the overall system security design, architecture, and other SSAA requirements against the concept of operations, operational environment, and threats to ensure that any risk to confidentiality, integrity, availability, or accountability of the system and associated data remains at acceptable levels.
- e. Roles and Responsibilities. In order to maintain this type accreditation, the host sites are responsible for ensuring compliance with the established configuration and carrying out their roles and responsibilities as identified in the SSAA.


COPY



f. Annual Compliance Validation: Conduct and report to the Certification Authority (CA) and CA Representative annual validation testing to ensure that the BSM-E BLSA Version 2.0 SSAA complies with security requirements, current threat assessment, and concept of operations. Ensure that the BSM-E BLSA Version 2.0 SSAA and associated BSM-E BLSA Version 2.0 Type Accreditation Checklist adequately address the functional environment into which BSM-E BLSA Version 2.0 resources have been placed.

This ATO is subject to immediate termination if there are any changes that adversely affect the security posture of the system. It is the responsibility of the J6F Director, BSM-E Program Manager, and the assigned BSM-E Information Assurance Manager to ensure that any change in threat, vulnerability, configuration, hardware, software, connectivity, or any other modification is analyzed to determine the impact on system security and reported to J-611. It is imperative that appropriate safeguards remain in place to maintain a level of security consistent with the requirements of this ATO.

Direct questions concerning this matter to Mr. James Haymaker, J-611, (703) 767-3100, or e-mail: ca.support@dla.mil.


MAE DE VINCENTIS
Director, Information Operations
Chief Information Officer